# Change Authority Board (CAB)
# Charter

## Charter Approval

| Approver | Title and/or Affiliation | Approval Date |
|---|---|---|
| Kris Hoffman | Chief Information Officer, DMDC and CAB Chairperson | |
| Rick Ongaro | Information Assurance Branch | |

## Table of Contents

## Purpose

The purpose of this charter is to establish the Defense Manpower Data Center (DMDC) Change Management CAB (Change Authority Board) and define its scope of authority, identify the membership and define their responsibilities.

## Scope

The DMDC CAB represents the interests of the Department of Defense (DoD) and the DMDC by ensuring that a structured process is used to consider the governance set forth by the DoD 8500.2, as well as to evaluate risk to the DMDC on select changes and releases brought to their attention. The CAB shall request that impact analysis of proposed changes be performed, review higher risk changes and releases, make decisions, and communicate decisions made to affected groups and individuals.

## Activities of the CAB

### Scheduled CAB Meetings

The CAB meets by default once per month. Any high risk and/or complex Release or Change must be presented to the meeting as determined by the associated Release or Change authority. Outside of scheduled monthly CAB meetings and by the direction of the CIO or the CAB chairperson, an emergency CAB meeting can be called with a minimum of one business days' notice.
Appendix A:
Appendix B: At the request of a stakeholder, a CAB meeting will be scheduled within one week of a requestor's notice.

### Emergency CAB Meeting

Occasionally, CAB meetings will be called on an ad hoc/emergency basis. Meeting agenda and minutes will still be captured. Decisions on proposed modifications will be arrived at as soon as possible. Any steps that were bypassed during the emergency will be completed as soon as possible or officially waived by the CAB at their next meeting.

### Meeting Activities

1. Agendas will be distributed as approved by the Chairperson. Items not contained in the agenda may be discussed, at the discretion of the CIO and/or the CAB Chairperson.
2. The review of previous CAB meeting action items
3. The review and disposition of proposed high risk modifications to DMDC configurations under direct control of the Mission Assurance policy DoD 8500.2
4. Ensure that reviewed IA issues, proposed releases or proposed changes will not have a negative impact on current DMDC operations.

5. Approve deviations from governing DoD 8500.2 policies or controls on a case-by-case basis.
6. Approve updated Change Management process modifications or modifications to Change Management process documentation.
7. Inform the DMDC Information Technology Steering Committee of any hardware/software configuration changes that affect the current Information Assurance or DMDC configuration standards and/or affect other organizations.
8. Meeting minutes and any action items will be distributed as approved by the Chairperson. Activities not contained in the minutes may be discussed, at the discretion of the CIO and/or the CAB Chairperson.

# CAB Membership

## Roles
## CAB Chairperson

The CAB Chairperson's responsibilities include the following but are not limited to:

1. Approves the CAB Agenda, including the determination of agenda items
2. Provides oversight of the Information Assurance program with regards to those areas specifically called out by the DoD 8500.2 and the Mission Assurance Category assigned to environments within the scope of the CABs authority.
3. Facilitates the CAB decision process for disposition of approved releases and changes brought before the CAB within the scope of the CABs authority. Decisions may be to approve, disapprove, defer, or send proposed changes back to the originator for rework.
4. Ensures that originators of proposed releases and changes are informed of decisions concerning disposition.
5. Directs DMDC release and change governance.

## Standing Members

CAB standing members will consist of representatives from the DMDC Information Assurance and other functional (business and technical) areas. These members will have voting privileges.

| DMDC Role or Organization | Name |
|---|---|
| CIO and CAB Chairperson | Kris Hoffman |
| Information Assurance Branch | Rick Ongaro |
| DMDC Change Management Process Owner | Denise McFaddin |
| | |

## Quorum

For a high risk decision the CAB is deemed assembled if at least 2/3 of the senior members (CIO, IAB and/or Division Directors) are present to come to an agreement on the IA area, the release or the change that is to be considered. In the event of a senior CAB member being unavailable they are to provide a delegate.

For all other risk considerations, any member of the CAB may review the proposed release or change if they are qualified to do so.

# Authority

The DMDC CAB derives its authority from the DoD 8500.1 and DoD 8500.2 policies and governance controls. The CCC will review each agenda item and/or proposed release or change against its real or perceived impact on the confidentiality, integrity and/or confidentiality of existing DMDC services and operations. The CAB has final recommendation over all issues brought before it for review. Any significant budget impacts will require Project Oversight Committee approval. CCC decisions are documented in the CCC minutes, and are implemented within the scope of its authority.

# Version Control

This DMDC Change Authority Board (CAB) charter supersedes all existing DMDC CAB charter in any previously published DMDC Change Management, TRB-CCB or Configuration Management documentation.

| Version | Date | Author | Change Description |
|---------|------|--------|--------------------|
| 1.0 | 9 Jan 2014 | Corde Wagner | Initial Version |

## Glossary

| Term/Acronyms | Definition |
|---------------|------------|
| Business Day | Generally Monday through Friday, 8 am to 5pm, not including approved holidays. |
| Change | The addition, modification or removal of anything identified as critical within the IT Configuration Baseline that could have an effect on IT Services. <br> Note: For purposes of DMDC policy and the Change Management process, all synonyms for change also apply. They include but are not limited to: modify, adjust, deploy, release, configure, modification, manipulate, transform, correct, add, remove, delete, alter, switch, tweak, update, patch, upgrade, etc. |
| Change Control Board (CCB) | A group of people that support the assessment, prioritization, authorization and scheduling of changes. A change control board is usually made up of representatives from: all areas within the IT service provider; the business; and |

| Term/Acronyms | Definition |
|---|---|
| | third parties such as suppliers.<br><br>The role of the Change Control Board (CCB) is to provide a policy review of proposed changes to ensure that the proposed changes increase the operational efficiency of the DMDC IT Infrastructure in support of the mission of DMDC. |
| Change Type | **Normal:** A change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process.<br>**Standard:** A pre-approved Change that is low risk, relatively common and follows a procedure or work instruction. For example, password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using the ticketing system.<br>**Emergency:** A change that must be introduced as soon as possible. For example:<br><ul><li>To resolve a major incident that is impacting production services</li><li>To implement a critical security patch in response to an active incident in the specified environment.</li></ul> |
| Change Request | CR: Change Request. Change Order ticket type within CA USD. (See Request for Change (RFC)) |
| Customer | Someone who receives goods or services from DMDC. |
| Change Windows | The defined period of time allowed for a change to be implemented. By best practices changes scheduled for a specific window of time must begin and end within that established change window.<br>Examples of Change Windows for DMDC is the "Static Maintenance Window" which is an approved time for STS changes to be performed. |
| Emergency Change Approvers | The ECA is a designated approval authority and subgroup of the Change Advisory Board (CAB) that makes decisions about emergency changes. |
| ITSM | IT Service Management: The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology. |
| Outage | Outage: Where a service is not available, during it's agreed Service Availability, to many or all users.<br><ul><li>An unstable condition, as involving an impending abrupt or unexpected disruption to production and/or to business service(s).</li><li>A stoppage in the functioning of a machine or mechanism due to a failure in the supply of power, electricity, data stream, etc.</li></ul> |
| Production | Production consists of all the assets and resources used to provide services to external and internal customers, including hardware, network, operating system |

| Term/Acronyms | Definition |
|---|---|
| | software, COTs software, customer facing business applications software (e.g. DEERS, RAPIDS, DAP, etc.), databases, and facilities (e.g. datacenter raised floors and other network/infrastructure rooms.) |
| Service | A means of delivering value to customers by facilitating outcomes customers want to achieve without ownership of specific costs and risks. |

## References

- DMDC Change Management TRB/CCB Procedure Document, v17,  August 2013
- DMDC Change Request Guidebook, November 2013
- DMDC Emergency-Change_Guidebook, November 2013
- DMDC Change Management Method of Procedure Guidebook, December 2013
- Management of the Department of Defense Information Enterprise, DoD Directive 8000.1, February 2009
- Recommended Security Controls for Federal Information Systems and Organizations, NIST 800-53 rev-4, National Institute of Standards and Technology, US Department of Commerce, 4/30/2013
- ISO/IEC 20000-1:2011, Clause 5
- ISO/IEC 20000-2:2012, Clause 9
- COBIT v5 Enabling Processes, ISACA, 2012
- ITIL Service Strategy, v3, TSO, 2011
- ITIL Service Transition, v3, TSO, 2011
- ITIL Service Operation, v3, TSO, 2011
- The Visible Ops Handbook, IT Process Institute, 2010